Naval War College

Newport, R.I.

Digital Deception: Implications of Pursuing Decision Superiority Using Deception in Cyberspace

By

Jerald L. Smith

A paper submitted to the Faculty of the Naval War College in satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal view and are not necessarily endorsed by the Naval War College or the Department of the Navy.

18 May 2001

Advisor:

Faculty Advisor
Donald W. Chisholm, Ph.D.

Report Documentation Page

Report Date 18052001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Digital Deception: Implications of Pursuing Decision Superiority Using Deception in Cyberspace	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Smith, Jerald L.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor’s Acronym(s)**
	Sponsor/Monitor’s Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 30	

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol:
C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

Digital Deception: Implications of Pursuing Decision Superiority Using Deception in Cyberspace

9. Personal Authors: Jerald L. Smith

10.Type of Report: FINAL

11. Date of Report: 18 May 2001

12.Page Count: 26 **12A Paper Advisor (if any):** Donald W. Chisholm, Ph.D.

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Military Deception, Cyberspace, Information Operations, Information Warfare, Information Superiority, Decision Superiority, Command & Control Warfare, Cognitive Hierarchy, Digital Deception, Asymmetric Warfare

15.Abstract:

Military Deception is one of the tools of Information Warfare (IW) and a key enabler of “Decision Superiority.” The next generation of military deception will include digital deception: deception in cyberspace. Joint Vision 2020 calls for U.S. Joint Forces to strive for, and obtain Decision Superiority as the goal of their Command and Control Warfare (C2W) efforts. The logical culmination of the pursuit of dominance across the cognitive hierarchy, Decision Superiority is the ability to make prudent military decisions while denying one’s adversaries the same.

What is deception’s role in the pursuit of Information and Decision Superiority? How does digital deception differ from traditional military deception? What advantages does it offer over traditional deception? What are the challenges to implementing deception in the digital domain? These are the questions addressed.

16.Distribution / Availability of Abstract:	**Unclassified** **X**	**Same As Rpt**	**DTIC Users**

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: (401) 841-6461

20.Office Symbol: **C**

Security Classification of This Page Unclassified

Professor of Joint Military Operations

Abstract

Military deception is one of the tools of Information Warfare (IW) and a key enabler of "Decision Superiority." The next generation of military deception will include digital deception: deception in cyberspace. Joint Vision 2020 calls for U.S. Joint Forces to strive for, and obtain Decision Superiority as the goal of their Command and Control Warfare (C2W) efforts. The logical culmination of the pursuit of dominance across the cognitive hierarchy, Decision Superiority is the ability to make prudent military decisions while denying one's adversaries the same.

What is deception's role in the pursuit of Information and Decision Superiority? How does digital deception differ from traditional military deception? What advantages does it offer over traditional deception? What are the challenges to implementing deception in the digital domain? These are the questions addressed.

Introduction

> *To secure ourselves against defeat lies in our own hands, but the opportunity of defeating an enemy is provided by the enemy himself.*
>
> *Sun Tzu*[1]

Joint Vision 2020 calls for U.S. Joint Forces to strive for, and obtain Decision Superiority as the goal of their Command and Control Warfare (C2W) efforts.[2] The logical culmination of the pursuit for dominance across the cognitive hierarchy, Decision Superiority is the ability to make prudent military decisions while denying one's adversaries the same. Military deception is one of the tools of Information Warfare (IW) and a key enabler of Decision Superiority. The latest form of deception, *digital deception*, (i.e., deception in cyber space), offers a means for today's combatant commander to not only defend against enemy Computer Network Attacks (CNAs), but to turn those attacks into offensive weapons. The next generation of military deception should include digital deception.

With the emergence of "the network" as a primary medium for storing and transmitting data and information, deception, which in and of itself is merely the passing of information, will take place within the digital domain. Deception in cyberspace poses unique challenges in its planning and execution: 1) Digital deception requires added coordination and deconfliction because it crosses the boundaries of four distinct but interrelated military doctrines, 2) The modern information environment is changing at a meteoric rate, 3) Information policies and laws are unclear and incomplete, and 4) The asymmetric nature of cyberspace activities collapses factor time while greatly increasing factors space and force.

The discussion that follows does not address the "mechanics" of designing and implementing deception (a subject thoroughly addressed in U.S. Joint Doctrine for Military Deception, Joint Pub 3-58), nor does it address the technical specifics of implementing digital deception (e.g., particular hardware, software, or network configurations: a subject requiring an advanced degree; or at least the vast experience of a teenage computer wizard).[3] The intent is to firmly establish in the reader's mind, an appreciation for:

1) How deception (traditional or digital) contributes to Information and Decision Superiority

2) The advantages of digital deception; particularly passive deception during a CNA

3) The challenges to planning and implementing digital deception

4) U.S. military doctrine affecting digital deception.

Superiority Across the Cognitive Scale

> *In order to achieve victory you must place yourself in your opponent's skin. If you don't understand yourself, you will lose one hundred percent of the time. If you understand yourself, you will win fifty percent of the time. If you understand yourself and your opponent, you will win one hundred percent of the time.*
>
> *Tsutomu Oshima*[4]

What exactly is Decision Superiority? World War II (WWII) offers an excellent example. In the Pacific Theater, the Japanese used analysis of past American operations and what they understood U.S. interests to be in order to simulate the American decision-making process. By analyzing the facts, they were able to envisage the plans that would best serve U.S. policy. *Although lacking intelligence information*, the Japanese were highly successful in forecasting Allied decisions. They accurately predicted the American plan for parallel advances across the

Pacific by Nimitz and MacArthur. They further predicted not only the islands on which the initial Allied invasion of the Japanese homeland would take place, but also the specific beaches to be breached. Incredibly, the Japanese successfully foretold the Allied plans *before* the Allies finalized what they would be.

Meanwhile, the United States and its allies were developing an elaborate deception operation, Operation PASTEL, to support the homeland invasion. PASTEL involved an extensive misinformation campaign, feigned air asset deployments, and phony supply drops to confuse the Japanese as to where and when the actual invasion would take place. However, based on *their knowledge and beliefs formed by past U.S. actions*, the Japanese fortified the correct areas and prepared a defense using the predicted U.S. plan as their blueprint. Even though the invasion of the Japanese homeland would never take place, one can conclude that the Allied deception plans were likely to have had marginal success in that the U.S. planners were unable to alter the *understanding* and *beliefs* of the Japanese. The Japanese enjoyed *Decision Superiority.*[5]

A basic overview of cognition will assist in understanding Japan's success in this example, and to lay the groundwork for successful deception: traditional and digital. Data, information, knowledge, and understanding are often treated as synonyms. They are in fact, descriptors of various stages of cognition: the evolution from raw data to information, information to knowledge, and knowledge to understanding. Data is individual measurements or observations. Information is data that is processed into a usable form: e.g., sorted, categorized, etc. Information assembled within a certain context becomes knowledge. Knowledge validated against a set of beliefs transforms to understanding.[6] Knowledge and understanding form the basis for making decisions.

Exploiting the cognitive hierarchy to gain Information and Decision Superiority is the focus of IO and Command and Control Warfare (C2W).

Attacking the lower end of the cognitive hierarchy has been the primary focus of IO and C2W during recent U.S. military operations. Neutralizing, if not destroying vital enemy Command and Control (C2) nodes received high priority during the initial phases of both Operation DESERT STORM[7] and Operation ALLIED FORCE.[8] Just as the Japanese observed the Allies during WWII, future adversaries are likely to analyze U.S. tactics and prepare accordingly. Merely denying the enemy access to information is likely to be insufficient to create the operational leverage sought from Information Superiority in future conflicts. Recognizing this fact, in *Joint Vision 2020* the Joint Chiefs of Staff warn against reliance solely on Information Superiority. They state: "Information Superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions."[9]

To obtain superiority at the upper end of the cognitive hierarchy, today's operational commander must not lose sight of the fact that able adversaries do not make decisions solely based on data processed into information. *Enemy decision-makers take into account the integrity of the information, the quality of the information, the significance of the information, and how that information correlates to their understanding of U.S. motives, processes, doctrine, and tactics*. "Knowledge Warfare" is warfare conducted against the upper levels of the cognitive model: knowledge and understanding. Achieving Decision Superiority is the ultimate goal of Knowledge Warfare. A primary means of invading the upper levels of the enemy's cognitive process is military deception.

The “Gentle Tao” of Deception[10]

When someone attacks you, he gives you a present of his strength.
To make use of this gift you must know how to receive it.
Yukiso Yamamoto[11]

Do not think of attack and defense as two separate things. An
attack will be a defense, and a defense must be an attack.
Kazuzo Kudo[12]

The Joint Chiefs define military deception as: “Those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission.”[13] Deception can be focused at national decision makers, military decision makers, and even the soldier in the trench. It is applicable at each level of war and across all phases of military operations.[14]

Historical use of deception by the United States combined misinformation with feigned troop movement and resource allocation to shape the enemy’s belief, that is, their perceived knowledge of U.S. intent. One of the most famous and successful military deceptions is Operation BODYGUARD. BODYGUARD was the elaborate set of deception operations conducted in preparation for the Normandy Invasion of WWII. It included feints into Scandinavia and the Balkans, and the establishment of an imaginary First U.S. Army Group (FUSAG) purportedly under the command of General George Patton. The FUSAG was to spearhead a notional invasion at Pas de Calais. Carefully misdirected operational fires and a faux FUSAG radio group transmitting deceptive radio traffic supported the illusion. This extensive deception, attributed as a key factor in the success of the invasion at Normandy, was based on Allied understanding of the Germans' belief that the invasion would take place at Pas de Calias. [15]

Modern military deception operations will include digital deception. Today, literally every aspect of the U.S. military is affected by world-wide-web and network-based information and knowledge systems. Through initiatives like the Army's *Force XXI* battlefield digitization initiative and the *Tactical Internet*; the Navy's Information Technology Vision (IT-21) and the *Navy-Marine Corps Intranet* (NMCI); and the Air Force's *Combat Information Transport System* (CITS) and the *Theater Battle Management Core System* (TBMCS); the U.S. military is pursuing the ability to: 1) Distribute combat information to soldiers, sailors, and airmen, providing them with enemy and friendly situational awareness, 2) Link deployed forces to their sustaining bases by means of a global information network to anticipate requirements and move materiel when and where it is needed, and 3) Implement information management processes and systems essential to *doing business on the Internet*.[16]

These significant investments in network-based information management emphasize the extent to which the U.S. military is reliant on the digital domain. Such reliance will certainly draw the attention of U.S. adversaries, creating an opportunity to exploit their attempts at gathering digital information. Newland observes: "While the US [*sic*] will enjoy information superiority over virtually any adversary we may face, it should never be assumed that we will be allowed to retain it or use it to full advantage. What information superiority really means is *being the one most* *dependent on computer and communications technology for combat success*" (emphasis mine).[17]

Digital deception does not differ from traditional deception with respect to its objective and design. It differs only in that the illusion is created in cyberspace. Digital deception can be a "stand-alone" operation, or an element of a more comprehensive deception plan in which other elements are also employed e.g., feints, demonstrations, psychological operations, etc.

Deceptive digital data and information can be passed to the enemy by either active or passive means. To pass the information actively, one would attempt to insert the information into the enemy's information environment. Active deception of this type would require "hacking" into enemy information systems. Passive deception takes advantage of the enemy's attempts to hack into one's own information environment and allows the capture of deceptive information. [18] This passive approach to deceptive information transfer is akin to the practice of self-defense using the philosophy of Judo.

> "When one is attacked by the enemy you do not oppose him. Instead you yield to him, just like the matador yields to the bull, and you use his strength and the principle of balance to bring about his downfall. Supposing, for example, there is a blow coming at me from a certain direction. Instead of defending myself, and pushing the blow off, the idea in judo is to carry the blow away. The knee goes out, catching the adversary below his point of balance, and he drops with a 'bang' brought about on his own initiative, and your cunning." [19]

Passive deception is particularly appealing in that the enemy does most of "the work." Allowing the adversary to work at gaining information establishes authenticity. Newland states that: "If at all possible, the enemy should be enticed to attack on our terms so that we can control what he accesses and lead him to believe he has succeeded.[20] Passive deception is attractive in that the adversary is the one conducting the CNA. As discussed in a following section, the legal aspects of conducting a CNA are considerable. Within the constraints of perfidy however, there are few restrictions on allowing a "hacker" to "take" deceptive information.

How can a CINC add digital deception as an arrow in his quiver and hardening to his or her armor? How can they facilitate the deception? What are the significant factors they must consider? These questions are considered below.

The Information Environment

> *Information Environment: The aggregate of individuals, organizations, and systems that collect, process, or disseminate information including the information itself.*
>
> *Joint Pub 3-13*[21]

Effective digital deception is only possible from within a highly capable information environment. The term "information environment" can easily be equated, erroneously, to Information Technology (IT). Based on the definition above, the information environment is composed of more than megabytes, baud rates, bandwidth, and operating systems. The information environment includes people: individuals and organizations with the expertise in, and mission of IO. How does the operational commander assemble the necessary hardware and software along with a team of skilled technologists so as to have in place the needed information environment? This is not an easy task.

Alberts, Garstka, and Stein report some sobering statistics with respect to IT capability growth rate (statistics are as of 1999):

1. Computer chip performance has doubled every 18 months for the past 45 years.[22]
2. Fiber optic cable transmission capacity doubles every 12 months.[23]

3. Data traffic over the Internet is doubling every 7.5 months.[24]
4. Voice traffic over the Internet core is doubling every 4 months.[25]

Given these growth rates, IT capability grows four fold during the average assignment of a combatant commander and the tours of the information technologists under his or her command. Under such conditions, it is unrealistic to expect a combatant command, increasingly reliant on *Net-Based Knowledge Acquisition and Control*, to maintain an effective IO team organically.[26] Recognizing this fact, centralized oversight and control of all military IO was recently assigned to the U.S. Space Command (USCINCSPACE). This new mission includes control of the Joint Information Operations Center that has the responsibility to facilitate, coordinate, and execute IO for the combatant commands. [27] As a supporting CINC, USCINCSPACE will coordinate the personnel, equipment, and processes necessary to conduct IO, including digital deception. Supported CINCs will likely depend on USCINCSPACE to coordinate with service component IO organizations and supporting organizations like DISA to establish a robust information environment in which U.S. information can be processed, transmitted and stored securely. USCINCSPACE will draw on the organic expertise that exists amongst the various service specific units dedicated to IO (e.g., The Air Force Information Warfare Center; the Navy Information Warfare Activity, the Fleet Information Warfare Center; and the Land Information Warfare Center), and the Defense Information Systems Agency (DISA). [28]

Computer Network Defense (CND) and offensive CNA will be tasks performed within the information environment. Treated as a specific “space,” (i.e., factor space), the information environment can be managed and defended using a Joint Task Force (JTF) approach just as with any other distinct space within a theater of operations. Recognizing the importance of computer network protection with respect to IO, USCINCSPACE, recently established a Joint Task Force for Computer Network Defense (JTF-CND).[29] Although not a campaign specific JTF, this task force can be assigned missions in support of the combatant commands, or conduct ongoing "generic" CND for U.S. operational forces. Each operation, each campaign, each theater requires a custom organization in which the information environment may be a minor consideration or a significant "space." As U.S. reliance on information technology and information networks grows, it is certainly possible that USCINCSPACE will become the supported CINC and the information environment will be the major theater of operations. Digital deception can be conducted, regardless of the organization of the information environment. Digital deception organization and planning are discussed in a later section.

National Information Policy, Information Law, and Deception

> *Yet today many Western democracies are in the position whereby it is legally easier for them to drop a laser guided bomb through an opponent's window, than crack into his computer system. Indeed legislators, and the public at large, as yet have failed to grasp the fact that another government cracking into a government computer, or putting a hacksaw through a fiber cable, is acting no differently than if they were shooting off a ballistic missile or lobbing a satchel charge into a munitions depot. It is an act of war, in every sense of the word.*
>
> *Carlo Kopp*[30]

It is only fitting that the rules, laws, and policies related to IO are as complex as the information environment for which they are written. Can IO be considered an act of war? Is IO an armed conflict? The DoD Office of General Counsel states:

> "It is by no means clear what information operations techniques will end up being considered to be "weapons," or what kinds of information operations will

> be considered to constitute armed conflict….If the deliberate actions of one belligerent cause injury, death, damage, and destruction to the military forces, citizens, and property of the other belligerent, those actions are likely to be judged by applying traditional law of war principles."[31]

The U.S. Justice Department however, maintains a different view:

> "It would be inappropriate for the Justice Department to offer comment, in response to the Defense Department's questions, on when a hack might legally constitute 'information warfare.' Rather, what we would say is this: unless an established predicate of international law (such as Article 51 of the U.N. Charter) has been met, the matter remains one for the law enforcement community, intelligence community, or both. And in most cases, our initial lack of information will demand that we presume that (1) the case is a criminal matter (as opposed to a national security case) and (2) the hacker is protected by the Fourth Amendment as well as the laws of the United States. These two presumptions are both necessary and practical because of the fundamental nature of networks and of network attacks and investigations."[32]

And lest the general public believe considerations of war are something for only the military to be concerned with, the DoD General Counsel also notes:

> "If combatant acts are conducted by unauthorized persons, their government may be in violation of the law of war, depending on the circumstances, and the individuals concerned are at least theoretically subject to criminal prosecution either by the enemy or by an international war crimes tribunal."[33]

At this point, IO Law is not clearly delineated. Although the precedence set by the "law of war" with respect to conventional means is valuable and even citable, IO raises many questions with few specific answers. The DoD Counsel concludes:

> "There seems to be little likelihood that the international legal system will soon generate a coherent body of 'information operations' law. The most useful approach to the international legal issues raised by information operations activities will continue to be to break out the separate elements and circumstances of particular planned activities and then to make an informed judgment as to how existing international legal principles are likely to apply to them. In some areas, such as the law of war, existing legal principles can be applied with considerable confidence. In other areas, such [as] the application of use of force principles to adopting an 'active defense,' it is much less clear where the international community will come out, and the result will probably depend more on the perceived equities of the situations in which the issues first arise in practice than on legal analysis. The growth of international law in

> these areas will be greatly influenced by what decision-makers say and do at those critical moments."[34]

Some aspects of the "law of war" are directly applicable to the planning and conduct of digital deception. Most notably, the concept of perfidy does not change. Digital deception cannot feign surrender, cease-fire, or armistice. It cannot camouflage deployment and maneuver using the veil of neutrality or the illusion of prisoner of war and medical activities. These restrictions are valid on the physical battlefield and within the digital domain.[35]

Preparation for deception may be ongoing, regardless of the CINC's status: at peace or at war. Within the constraints of current legal information law, and using the best available intelligence, deception mechanisms, including actual interactions with potential targets may be needed, *before* hostilities occur. Preparing the illusion and gaining the trust of the target may occur at the boundaries of the IO legal framework.

The message to the combatant commander is: IO presents a unique legal challenge. Because IO law is in a state of flux, the CINC must ensure their legal counsel remains current on IO law evolution in order to employ effective IO and stay within the legal constraints of the day. As CINCs plan IO activities, including deception, they should ensure that legal counsel is an active member of the planning of those efforts and that procedures are in place to ensure legal counsel review is obtained as IO occurs so that all operations remain within the constraints of the law.[36]

The Asymmetric Threat

> *… we teach the pupil to act on the fundamental principles of Judo, no matter how physically inferior his opponent may seem to him, and even if by sheer strength he can easily overcome him; because if he acts contrary to principle his opponent will never be convinced of defeat, no matter what brute strength he may have used.*
>
> *Jigoro Kano*[37]

Asymmetric warfare can be characterized as the use of unusual, unexpected, and unpredictable strategies, operations, and tactics to offset a military power imbalance between adversaries. As the sole military superpower, the U.S. can expect virtually all adversaries to utilize asymmetric techniques.[38] Cyberspace is an enabler of asymmetric warfare. Newland observes:

> "IW is a sort of "Charles Atlas in a pill," an immediate equalizer. To assume information dominance and automatic information superiority simply because of superpower status is the height of arrogance. Even the smallest, poorest country can find the resources to fund intrusions, computer viruses, logic bombs and system manipulation in the global Internet to which the US military's C4I structure is not only attached but embedded. It may not even be a country that funds such activity. The major threat may be asymmetric in nature."[39]

The U.S. can expect the expanse of potential adversaries to rapidly grow with the success and relative ease of implementation of asymmetric strategies and tactics. Lind and others observe that the next generation of warfare, what they refer to as "Fourth Generation Warfare," will likely see a battlefield that will "include the whole of the enemy's society."[40] They further observe: "…fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between 'civilian' and 'military' may disappear."[41]

In the aftermath of the "downing" by China of a U.S. EP-3 reconnaissance aircraft in April 2001, the Washington Times reported the following:

> "Computer-savvy citizens of both China and the United States have begun their own war on the Internet as relations between the two powers continue to deteriorate.
>
> American hackers are urging each other to break into Web sites hosted in China, and they say that U.S. hackers have already penetrated hundreds of Chinese Webs sites. Chinese hackers are vowing to retaliate with a weeklong attack on U.S.-based Web sites and computer networks…"[42]

In this example, who is the target for C2W efforts? Is it: The Chinese Military? The Chinese Government? A dissident Chinese organization? The Chinese population at large? And what of the U.S. hackers conducting unauthorized and probable illegal IO? The target could reside in any or all. Are China and the United States at peace or at war? What are the legal implications of conducting C2W against the threatened attacks? Operating in Cyberspace, factor time approaches zero, factor space expands to virtually the entire world, and factor force is arguably only limited by the availability of a personal computer and a connection to the Internet. It is easy to conclude that asymmetric warfare levels the Information Superiority battlefield.

Intelligence and timing are key to the combatant commander's ability to conduct deception in an asymmetric theater of operations. The field-of-view for intelligence efforts must widen to consider the full extent of potential adversaries in the CINC's area of responsibility. The CINC's intelligence organization must be prepared for quick reaction. In an asymmetric theater; adversaries will emerge, depart, and transform to a given situation with lightening fast response. Intelligence support in such an environment is no small task, and if considered critical in traditional deception, becomes vital in digital deception.

Doctrine and The Principles of Deception for the Digital Domain

> *…the control of a deceptive operation must be decided upon the self-evident principle that no people can safely tell the same lie to the same person except by closely concerted action.*
>
> *R.F. Hesketh*[43]

What doctrine applies when planning and implementing digital deception? Digital deception is an element of Military Deception, C2W, IO, and C4. Effective digital deception will require significant coordination between the operational planners assigned to each of these areas.

Joint doctrine for IO states: "IO requires *early integration between components, groups, organizations, and agencies* involved in planning and executing IO actions and activities" (emphasis mine).[44] Doctrine for C2W and Military Deception has similar statements emphasizing the importance of coordination.[45] Although not specifically identified in U.S. Joint C4 doctrine, digital deception will utilize C4 assets and be tied to the overall C4 infrastructure. Coordination with the overseers of the C4 system is imperative lest the deceiver becomes the deceived.

U. S. doctrine for military deception as defined in Joint Pub 3-58 identifies six principles of military deception: Focus, Objective, Centralized Control, Security, Timeliness, and Integration.[46] Certain characteristics of digital deception are of interest when considering each of the principles.

Focus

As with traditional deception, an adversary decision maker must be the target. Joint Pub 3-58 states: "The adversary's intelligence system is normally not the target. It is only the primary conduit used by deceivers to get selected information to the decision maker."[47] A digital deception corollary to this pronouncement is: The information environment is normally not the target. It is only the conduit used to get selected information to the targeted decision maker.

Objective

The objective of deception, digital or otherwise, is to achieve a desired enemy decision. Whether that decision is strategic, operational, or tactical in nature determines at which level of war the deception is associated and who the specific target will be. Therefore, deception planning at the highest level begins with identifying the desired decision, which leads to the choice of one or more targets that will either make or influence the decision. Once the target(s) are identified, their understanding and beliefs are assessed to determine the design of the deception (e.g., physical, digital, etc.). Accurate, detailed intelligence is the key to the success of deception. The more that is known of the target, their education, experience, motivations, and values, the easier it is to gain their trust through the illusion. If digital deception is to be used, specific questions to be asked include: What trust does the target place in digital information? What are their perceptions of cyberspace? Their biases? What will create a sense of integrity regarding the deceptive information to be passed on?

Centralized Control

During WWII, the London Controlling Section (LCS) was the first organization established at the operational level with the sole purpose of planning deception strategies. Winston Churchill personally oversaw its design and participated in its actions.[48] The need for centralized control of digital deception efforts is only magnified by the complexities associated with operating across multiple doctrines.

Security

Churchill observed: "In war time, truth is so precious that she should always be attended by a bodyguard of lies."[49] Ensuring the security of the deception, its intent, its means, its mere existence, is critical in maintaining the trust of the target. Equally as important, the security of the intelligence sources that feed the deception is paramount. Because Churchill prized his possession of the German Enigma machine so highly, he directed no action be taken in response to decoded intercepts unless cover could be provided.[50] He went as far as to repeatedly allow naval convoys to come under U-boat attack rather than risk compromising the fact that he could break the German codes.[51]

The complexity of protecting digital deception plans is elevated because of the increased amount of coordination required to take place between the various operational elements. *The pyramid of potential security breeches grows geometrically with each and every "need-to-know" element entrusted with the deception plan*.

Timeliness

Deception timing presents a dichotomy with respect to the nature of cyber operations and the need to create a trust relationship with the target. Factor time collapses in cyberspace. On the other hand, planning deception and operating to gain the trust of the target demands time. Hesketh observed: "Although there may be occasions when its [deception] services can be usefully enlisted to give immediate aid, it is generally more correct to regard it as a method which achieves its results by a slow and gradual process rather than by lightning strikes. Like the fly-wheel of an engine, it requires time to gain momentum and time again to lose it."[52]

To establish the requisite trust, the wheels of deception may need to be set in motion before the target is clearly defined and the operation planned. This magnifies the need for a constant flow of intelligence to the CINC so that deception contingencies can be considered. Within the assigned area of operation, who are the potential threats? How can they be deceived? What IO can be conducted during peacetime to expedite the initiation of deception when conflict arises? What are the legal constraints that bound IO and deception activities in and out of war? These are all questions to be pursued routinely to facilitate efficient and effective IO including digital deception.

Integration

"Each deception must be fully integrated with the basic operation it is supporting. [To ensure it is deconflicted with other aspects and phases of the operation.] The development of the deception concept must occur as part of the development of the commander's concept of operations. Deception planning should occur simultaneously with operation planning."[53]

Because of the extensive reliance on information and network-based operations by U.S. operational forces, an IO planning cell reporting directly to the J3 is advisable. Within the IO planning cell, a cell for digital deception is needed to assign roles, responsibilities, levels of authority, and support requirements for the digital deception, and to ensure all entities within the JTF affected by the planned deception are aware of the operation and how it relates to their area of responsibility. An obvious choice to lead digital deception planning is the newly established JTF-CND. Arguably, digital deception is a form of CND, and as an element of the overall combatant command with IO responsibility (i.e., USCINCSPACE), the JTF is ideally situated to coordinate digital deception plans with the overall IO effort. On the CINC staff, Special Technical Operations

(STO) has the "Big Picture" insight across the activities of the CINC to ensure necessary coordination occurs and should represent the CINC during digital deception planning.

The nuances of the principles of deception when utilizing cyberspace are subtle. They do not necessarily determine the ability to conduct digital deception, but they certainly drive the quality of the deception and the ease of implementing the deception.

Conclusions

> *I make the enemy see my strengths as weakness and my weaknesses as strengths while I cause his strengths to become weaknesses and discover where he is not strong.*
>
> *Sun Tzu*[54]

> *All warfare is based upon deception.*
>
> *Sun Tzu*[55]

Digital deception is a viable and inevitable tool for the operational commander. Deception operations in the digital domain, although at their core, the same as other deception activity, do call for special considerations. The information environment is complex and dynamic. Digital deception, and IO in general are cutting new ground with respect to international law. U.S. information policies, and agency roles and responsibilities are murky at best. The asymmetric threat increases the C2W target set, collapses factor time, and magnifies factors space and force. Digital deception spans a number of critical U.S. military doctrines without specific consideration in any.

Conducted effectively, digital deception can be a “multiplier,” a deception multiplier. When one considers the depth to which IO permeates into all aspects of military operations, deception in cyberspace gives the combatant commander the ability to develop deception in areas possibly not practical to pursue in the physical realm. Granted, some level of physical activity will be required to authenticate the digital deception. However, once authenticity is established, the scope of a deception in cyberspace can greatly exceed the physical resource limitations an operation. Effective digital deception offers the potential of being a key enabling factor in the U.S. pursuit of dominance across the cognitive hierarchy.

Notes

[1] Sun Tzu; quoted in Neil Ohlenkamp, "Words of Wisdom on Learning Judo," 20 January 2000, JudoInfo Online Dojo, <http://JudoInfo.com/quotes.htm> [23 April 2001], 3.

[2] U.S. Joint Chiefs of Staff, "Joint Vision 2020," June 2000, Joint Electronic Library CD-ROM, Washington DC: Joint Chiefs of Staff, August 2000, 8.

[3] U.S. Joint Chiefs of Staff, Joint Doctrine for Military Deception, Joint Pub 3-58 (Washington DC: 31 May 1996).

[4] Tsutomu Oshima; quoted in Ohlenkamp, 4.

[5] The example of Japanese efforts to discern Allied intent during WWII is based on information drawn from the work of Thomas H. Huber in his analysis of Operation PASTEL. Thomas H. Huber, Pastel: Deception in the Invasion of Japan (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College Combat Studies Institute, 1988), 35-41.

[6] U.S. Joint Chiefs of Staff, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, Joint Pub 6-0 (Washington DC: 30 May 1995), I-4.

[7] James McLendon, "Chapter 7: Information Warfare: Impacts and Concerns," Barry R. Schneider and Lawrence E. Grinter, Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Security No.3, rev. (Maxwell Air Force Base, AL: Air University Press, 1998), 187; Department of Defense, Conduct of the Persian Gulf War, Final Report to Congress (Washington DC: April 1992), 126-128.

[8] Department of Defense, Kosovo/Operation Allied Force After-Action Report, Report to Congress (Washington DC: 31 January 2000), 7.

[9] U.S. Joint Chiefs of Staff, "Joint Vision 2020," 8.

[10] Drawn from Watts' use of the term "The Gentle Tao" in his article on Judo. Alan Watts, "Judo: The Gentle Tao," 4 February 2001, JudoInfo Online Dojo, <http://JudoInfo.com/wattss.htm> [23 April 2001].

[11] Yukiso Yamamoto; quoted in Ohlenkamp, 4.

[12] Kazuzo Kudo; quoted in Ohlenkamp, 6.

[13] U.S. Joint Chiefs of Staff, Joint Pub 3-58, v.

[14] Ibid., I-1.

[15] McLendon, 180-181.

[16] Gregory Slabodkin, “Tactical Internet,” Military Information Technology, vol. 3: issue 5, October 1999, 24-25; Edward J. Walsh, “Business Unusual,” Military Information Technology, vol. 4: issue 5, July 2000, 6; Gregory Slabodkin, “Information Superhighway,” Military Information Technology, vol. 3: issue 4, 1999, 56-58; William Miller, “C2’s Giant Step Forward,” Military Information Technology, vol. 5: issue 3, April 2001, 34-36.

[17] Ronald K. Newland, “Tactical Deception In Information Warfare – A New Paradigm For C4i,” Journal of Electronic Defense, vol. 21, no. 12, December 1998, 46.

[18] Ronald K. Newland, 48.

[19] Watts.

[20] Newland, 48.

[21] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington DC: 9 October 1998), I-9.

[22] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare – Developing and Leveraging Information Superiority, 2d ed., rev., (Washington D.C.: Department of Defense C4ISR Cooperative Research Program, 1999), 247.

[23] Ibid., 249.

[24] Ibid., 251.

[25] Ibid.

[26] *Net-Based Knowledge Acquisition* is a term suggested by Dr. Donald Chisholm, Professor of Joint Maritime Operations, Naval War College, Newport, RI.

[27] Major General James D. Bryan; interviewed by JoAnn Sperber, “Cyber Defender Q&A,” Military Information Technology, vol. 5: issue 3, April 2001, 25.

[28] Brian Fredericks, “Information Warfare: The Organizational Dimension,” 1996, Institute for National Strategic Studies Sun Tzu Art of War in Information Warfare Compendium, <http://www.ndu/edu/inss/siws/fore.html> [28 April 2001], 4-11; Defense Information Systems Agency, “DISA Mission and Mandate,” Defense Information Systems Agency Official Web Site, 15 December 2000, <http://www.disa.mil/missman.html> [28 April 2001]

[29] Sperber, 25.

[30] Carlo Kopp, “Part 1- A fundamental Paradigm of Infowar,” February 2000, Information Warfare, <http//www.infoware.com/info_ops/00/info_ops033000b_j.shtml> [22 April 2001], 11.

[31] U.S. Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations, 2d ed., (Washington DC: 1999), 6-7.

[32] Scott Charney, Chief, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Justice Department, to Judy Miller, General Counsel, Department of Defense, (Washington DC: 11 August 1999), 4.

[33] U.S. Department of Defense Office of General Counsel, 7.

[34] Ibid., 47.

[35] U.S. Department of the Navy-Naval Doctrine Command, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-2.1/COMDTPUB P5800.7 (Norkolk, VA: October 1995), 12: 1-2.

[36] U.S. Department of Defense Office of General Counsel, 47.

[37] Jigoro Kano; quoted in Ohlenkamp, 3.

[38] David L. Grange, "Asymmetric Warfare: Old Method, New Concern," ROA National Security Report, The Defense Education Trust Fund of the Reserve Officers Association of the United States (Washington D.C.: March 2001; reprint National Strategy Forum Review, Winter 2000), 29.

[39] Newland, 45.

[40] William S. Lind and others, "The Changing Face of War: Into the Fourth Generation," October 1989, Marine Corps Gazette, vol. 73, no. 10, October 1989, 25.

[41] Ibid., 23.

[42] Agence France-Presse, "China warns of coming hack attack: Retaliatory assault on U.S. computers planned for May," Washington Times, 23 April 2001, sec. A, 1.

[43] R.F. Hesketh, Fortitude: A History of Strategic Deception in North Western Europe April, 1943 to May, 1945, unpublished after-action history of deception operations in north-west Europe, primarily those preceding the invasion of Normandy, February 1949, 259 pages, quoted in Michael I. Handel, ed., Strategic And Operational Deception In The Second World War (Totowa, NJ: Frank Cass & Co. LTD., 1987), 21.

[44] U.S. Joint Chiefs of Staff, Joint Pub 3-13, V-4.

[45] U.S. Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington DC: 7 February 1996), IV-1; Joint Pub 3-58, III-1.

[46] U.S. Joint Chiefs of Staff, Joint Pub 3-58, I-3.

[47] Ibid., I-3.

[48] McLendon, 178.

[49] Sir Winston Churchill, quoted in Anthony Cave Brown, Bodyguard of Lies (New York: Harper & Row, 1975): 10; in McLendon, 195.

[50] David Kahn, Seizing the ENIGMA: The Race to Break the German U-Boat Codes, 1939-1943 (Boston: Houghton Mifflin Co., 1991: 276, in James McLendon, "Chapter 7: Information Warfare: Impacts and Concerns," Barry R. Schneider and Lawrence E. Grinter, Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Security No.3, rev. ed. (Maxwell Air Force Base, AL: Air University Press, 1998), 178.

[51] James L. Gilbert and John P. Ginnegan, eds., U.S. Army Signals Intelligence in World War II: A Documentary History, Center of Military History, United States Army (Washington DC, GPO, 1993): 175, in James McLendon, "Chapter 7: Information Warfare: Impacts and Concerns," Barry R. Schneider and Lawrence E. Grinter, Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Security No.3, rev. ed. (Maxwell Air Force Base, AL: Air University Press, 1998), 178.

[52] R.F. Hesketh, Fortitude: A History of Strategic Deception in North Western Europe April, 1943 to May, 1945, unpublished after-action history of deception operations in north-west Europe, primarily those preceding the invasion of Normandy, February 1949, 259 pages, quoted in Michael I. Handel, ed., Strategic And Operational Deception In The Second World War (Totowa, NJ: Frank Cass & Co. LTD., 1987), 27.

[53] U.S. Joint Chiefs of Staff, Joint Pub 3-58., I-3.

[54] Sun Tzu, The Art of War, quoted in Scott Gerwehr and Russel W. Glenn, "The art of Darkness: Deception and Urban Operations, 2000," Rand Publications, <http://www.rand.org/publications/MR/MR1132/> [11 April 2001], 19.

[55] Ibid., 15.

Bibliography

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare – Developing and Leveraging Information Superiority, 2d ed., rev. Washington D.C.: Department of Defense C4ISR Cooperative Research Program, 1999.

Brown, Anthony Cave. Bodyguard of Lies. New York: Harper & Row, 1975.

Charney, Scott, Chief, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Justice Department, to Judy Miller, General Counsel, Department of Defense. 11 August 1999. Washington DC

Defense Information Systems Agency. "DISA Mission and Mandate." Defense Information Systems Agency Official Web Site. 15 December 2000. <http://www.disa.mil/missman.html> [28 April 2001].

Fredericks, Brian. "Information Warfare: The Organizational Dimension." 1996. Institute for National Strategic Studies Sun Tzu Art of War in Information Warfare Compendium. <http://www.ndu/edu/inss/siws/fore.html> [28 April 2001].

Gilbert, James L. and John P. Ginnegan. eds. U.S. Army Signals Intelligence in World War II: A Documentary History. Center of Military History, United States Army. Washington DC: GPO, 1993.

Grange, David L. "Asymmetric Warfare: Old Method, New Concern," ROA National Security Report, The Defense Education Trust Fund of the Reserve Officers Association of the United States. Washington DC: (March 2001): 29.

Handel, Michael I. ed. Strategic And Operational Deception In The Second World War Totowa. NJ: Frank Cass & Co. LTD., 1987.

Huber, Thomas M. Pastel: Deception in the Invasion of Japan. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College Combat Studies Institute, 1988.

Kahn, David. Seizing the ENIGMA: The Race to Break the German U-Boat Codes, 1939-1943. Boston: Houghton Mifflin Co., 1991.

Kopp, Carlo. "Part 1- A fundamental Paradigm of Infowar." February 2000. Information Warfare. <http//www.infoware.com/info_ops/00/info_ops033000b_j.shtml> [22 April 2001].

Lind, William S., Keith Nightengale, John F. Schmitt, Joseph w. Sutton, and Gary I. Wilson. "The Changing Face of War: Into the Fourth Generation." October 1989. Marine Corps Gazette, vol. 73, no. 10, (October 1989): 25.

Miller, William. "C2's Giant Step Forward," Military Information Technology, vol. 5: issue 3, (April 2001): 34-36.

Newland, Ronald K. "Tactical Deception In Information Warfare – A New Paradigm For C4i." Journal of Electronic Defense, vol. 21, no. 12, (December 1998): 43-48.

Ohlenkamp, Neil. "Words of Wisdom on Learning Judo." 20 January 2000. JudoInfo Online Dojo. <http://JudoInfo.com/quotes.htm> [23 April 2001].

Schneider, Barry R. and Lawrence E. Grinter. Battlefield of the Future - 21st Century Warfare Issues. Air War College Studies in National Security No.3 rev. Maxwell Air Force Base, AL: Air University Press, 1998.

Slabodkin, Gregory. "Information Superhighway," Military Information Technology, vol. 3: issue 4, (1999): 56-58.

________. "Tactical Internet," Military Information Technology, vol. 3: issue 5, (October 1999): 24-25.

Sperber, JoAnn. "Cyber Defender Q&A," Military Information Technology, vol. 5: issue 3, (April 2001): 25-29.

U.S. Department of Defense. Conduct of the Persian Gulf War. Final Report to Congress. Washington DC: April 1992.

________. Kosovo/Operation Allied Force After-Action Report. Report to Congress. Washington DC: 31 January 2000.

U.S. Department of Defense Office of General Counsel. An Assessment of International Legal Issues in Information Operations, 2d ed. Washington DC: 1999.

U.S. Department of the Navy-Naval Doctrine Command. The Commander's Handbook on the Law of Naval Operations. NWP 1-14M/MCWP 5-2.1/COMDTPUB P5800.7. Norkolk, VA: October 1995.

U.S. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington DC: U.S. Joint Chiefs of Staff, 30 May 1995.

________. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington DC: U.S. Joint Chiefs of Staff, 7 February 1998.

________. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington DC: U.S. Joint Chiefs of Staff, 9 October 1998.

________. Joint Doctrine for Military Deception. Joint Pub 3-58. Washington DC: U.S. Joint Chiefs of Staff, 31 May 1996.

________. "Joint Vision 2020." June 2000, Joint Electronic Library CD-ROM. Washington DC: U.S. Joint Chiefs of Staff, August 2000.

Walsh, Edward J. "Business Unusual," Military Information Technology, vol. 4: issue 5, (July 2000): 6.

Watts, Alan. "Judo: The Gentle Tao." 4 February 2001. JudoInfo Online Dojo. <http://JudoInfo.com/wattss.htm> [23 April 2001].